Chapter 1
SDLC Handbook Introduction and Tailoring

Chapter Overview

This chapter states:

- The purpose and scope of the Information Technology (IT) Systems Development Life Cycle (SDLC) process that must be followed within the United States Customs Service
- The principles and standards that form the basis of the Systems Development Life Cycle process
- The organization of this handbook

The concepts, policies, and standards presented in this chapter apply to ALL Customs Automated Information System (AIS) projects regardless of project size, methodology, or technology used.

In This Chapter

Section A
SDLC Handbook Organization and Processes

Purpose of the SDLC Handbook

The U.S. Customs Service has made a commitment to the General Accounting Office (GAO) to reach Level 3 of the Software Engineering Institute's (SEI's) Capability Maturity Model (CMM) for Software Engineering by 2003. With that goal in mind, the purpose of this handbook is to describe and define the life cycles and methodologies approved for use by the United States Customs Service.

Handbook Scope

This handbook is intended to be a primary reference for Customs Automated Information Systems (AIS) users, project managers, and developers who build and maintain quality systems. If you adhere to the guidance in this handbook, you will be in compliance with applicable Federal and industry standards.

This handbook applies to the following groups:

- Everyone involved in the AIS development process, regardless of their experience level and/or position
- All systems and applications (including local AIS) developed by or for the United States Customs Service
- All systems and applications used by Customs employees and contract personnel, other government agencies, persons or companies using Customs resources, whether or not under direct control of the Office of Information and Technology (OIT) relating to SDLC processes

In This Section

SDLC Handbook Organization

Volumes

For ease of handling, these materials are divided into two volumes.

- Volume I contains materials related to processes and project controls. These are materials that would tend to be used more by a project manager; however, all project team members should be familiar with these contents.

- Volume II contains the materials related to life cycles and the approved document templates. These materials would be used more by system developers in the performance of their tasks.

Chapters 1, 2, 12, and 17 contain information that applies equally to both types of handbook users. Therefore, they are included in both volumes.
Appendix A is also included in both volumes.

Parts of the SDLC Handbook

This SDLC Handbook is divided into four parts, based on the types of materials in each part:

- Part I - Navigation and Processes, Chapters 1-5
- Part II - Life Cycles and Methodologies, Chapters 6-11
- Part III - Document Templates and Guidelines, Chapters 12-17
- Part IV - Glossaries and References, Appendices A-B

Navigation and Processes

Part I consists of chapters which provide information on:

- The overall processes used in the system development life cycle
- Management activities, deliverables, and processes
- Guidelines for adapting and using this SDLC Handbook

Continued on next page

SDLC Handbook Organization, Continued

Life Cycles and Methodologies

Part II consists of descriptions of the approved Customs Life Cycles and development methodologies. For each path, these descriptions include the:

- Logical project phases
- Activities performed in each phase
- List of Documentation

Note: In all cases, the SDLC process followed by a project may be iterative; that is, a life-cycle phase may be repeated or reentered from a succeeding phase as often as necessary to ensure the delivery of a good system.

Document Templates and Guidelines

The chapters in Part III describe each of the specific documents in detail, usually providing both a Table of Contents and descriptions of the required information. These documents may be tailored as defined in Volume I, Chapter 1, Section C, *Tailoring Guidelines*, depending on a project's needs, life cycle, and methodologies.

Volume I, Chapter 12, *SDLC Deliverables Summary Tables*, provides overall matrices of the SDLC documents including information on the SDLC life cycle phases in which each document is created, revised, and finalized.

Glossaries and References

Part IV consists of the Handbook Appendices including Terms Used in this Handbook (including Project Roles and Definitions) and Reference Sources.

Continued on next page

SDLC Handbook Organization, Continued

Roadmaps

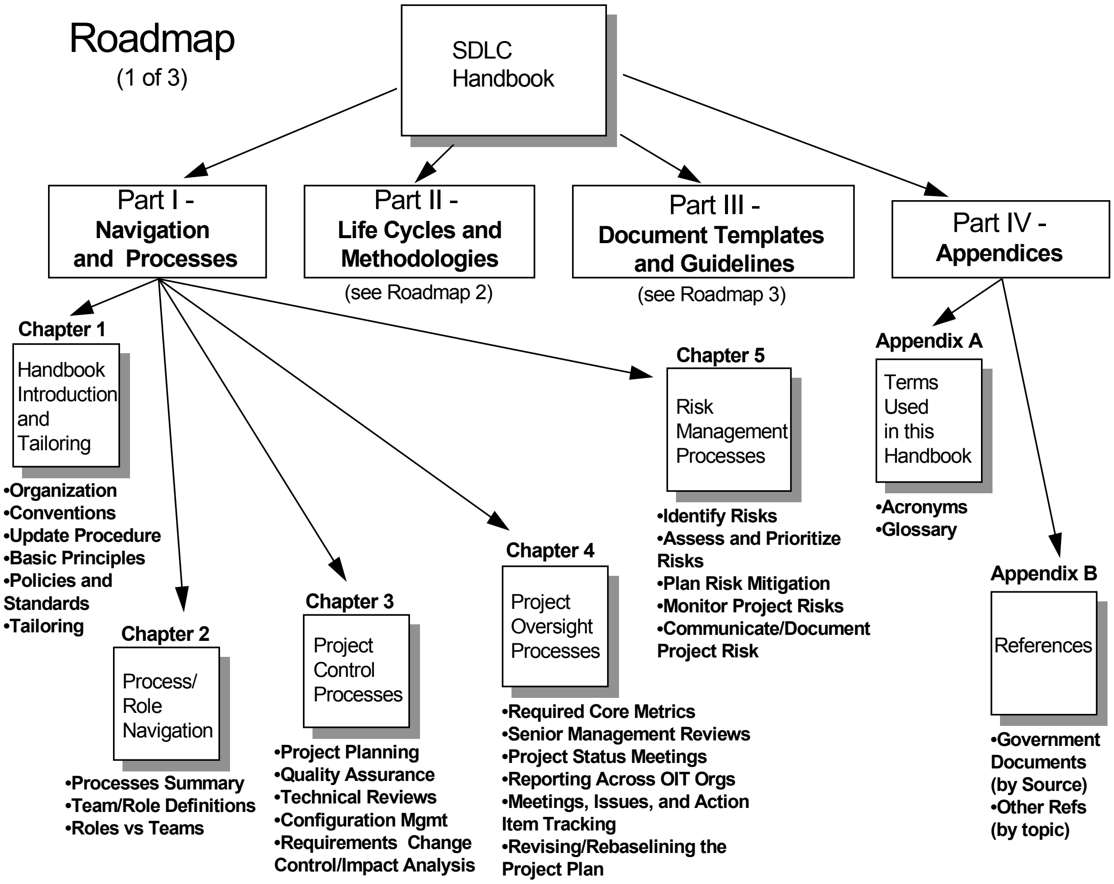
The following roadmap diagrams illustrate the main topics discussed in sections of each chapter. These pages can be used as a pullout guide to the handbook.

Volume References

On this diagram, all chapters in Part I (Chapters 1-5) and both those in Part IV (Appendices A and B) appear in Volume I.

Chapters 1, 2 and Appendix A also appear in Volume II.

**Roadma
p
Diagram**



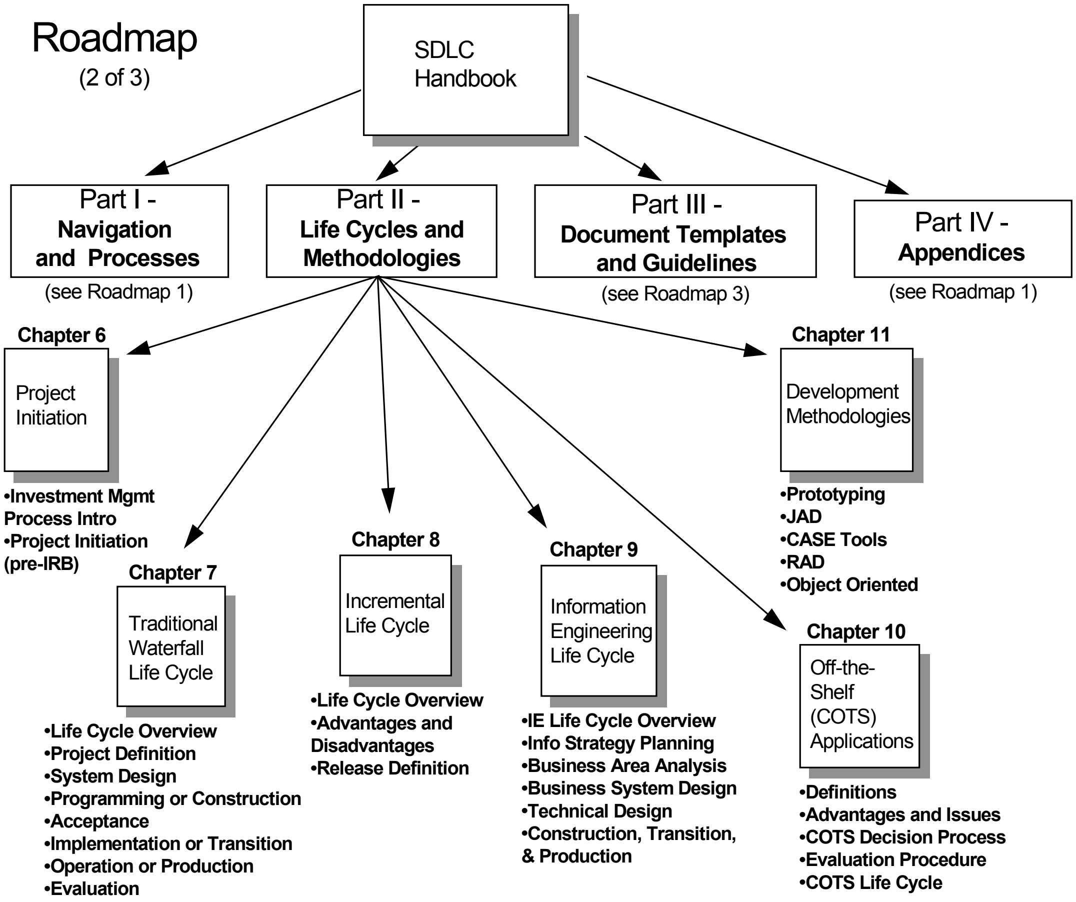
Continued on next page

SDLC Handbook Organization, Continued

Volume Reference

On this diagram, Part II Chapters 6 and 11 appear in Volume I and Chapters 7-10 appear in Volume II.

Roadmap Diagram (continued)



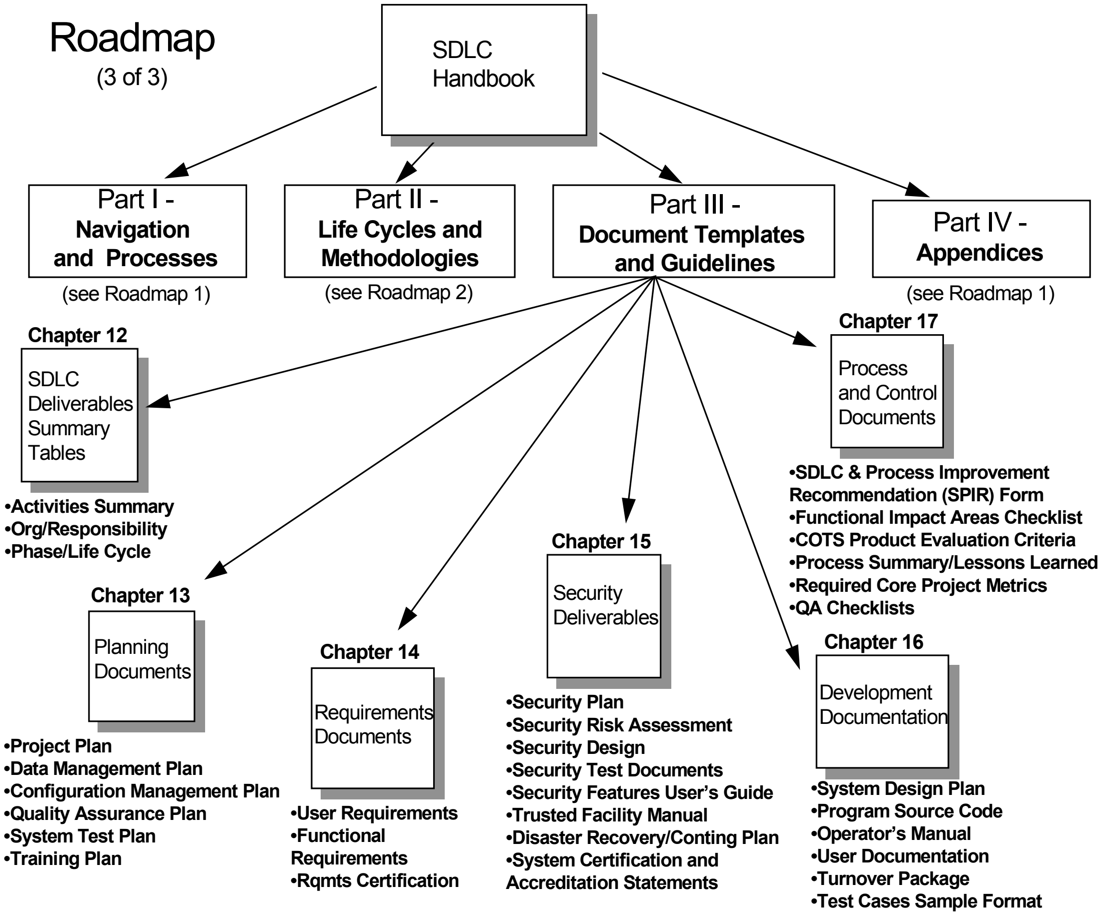
Continued on next page

SDLC Handbook Organization, Continued

Volume Reference

On this diagram, all chapters in Part III (Chapters 12-17) appear in Volume 2. Chapters 12 and 17 also appear in Volume 1.

Roadmap Diagram (continued)



SDLC Handbook Conventions

Purpose

The conventions discussed below are used throughout this handbook.

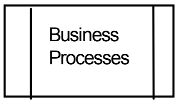
Format

This handbook has been prepared using the Information Mapping® formatting. This format includes:

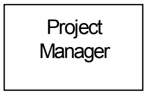
- Tables of Contents for each chapter and section, as well as a table of contents for the document as a whole.
- Chapter and Section titles, centered at the beginning of each unit
- Topic heading on each page
- Topic key words at the left hand margin

Process Flow Diagram Conventions

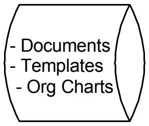
The following conventions are used to depict the processes, activities, organization groups or roles, primarily roles, automated systems, and information flows in the process and activity diagrams.



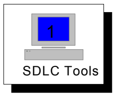
Input or Output Process Block Example



Organization Group or Role Block Example



Data and Document Repository Block Example



Automated System Block

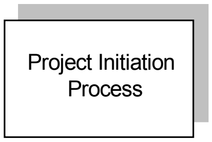
Business
Sponsor

Primary Role

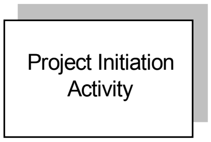
Continued on next page

SDLC Handbook Conventions, Continued

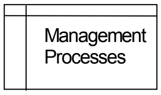
Process Flow Process Flow Diagram Conventions (continued)



Process Being Depicted



Activity Being Depicted



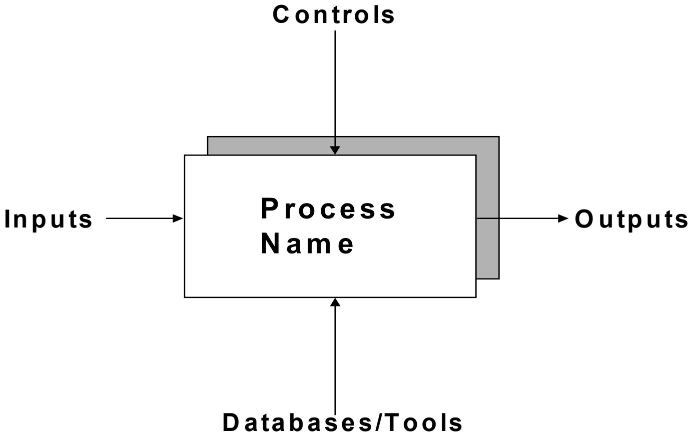
Management Processes

→

Information Flow Direction

Process Flow Diagram Box Conventions

In addition, the Process Flow Diagram itself has a format convention which identifies how the information appears around the center process box.

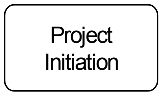


Continued on next page

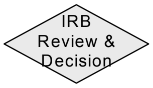
Handbook Conventions, Continued

Life Cycle Flow Diagram Conventions

The following conventions are used to depict the life cycle flows and the deliverables at each stage:



Step in the Life Cycle



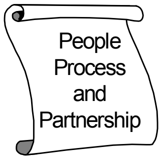
An Investment Review Board Decision Point

User & Functional Requirements
Project Plan
Disaster Recovery Plan
Data Management Plan
Risk Assessment - Security Plan
System Test Plan
Security Test Plan
Trusted Facility Manual
Configuration Management Plan
Quality Assurance Plan

Deliverables Block

***Bolded* Deliverables Should Be Reviewed and/or Revised As Necessary**

Deliverables in Regular Font are begun in this Step



People, Process and Partnership, Customs strategic long-range process plan.

Process Description Conventions

In order to meet ‘best practice’ guidelines for a “well-defined process”, the sections describing an SDLC process or procedure usually contain both textual and graphic representations of the process and must, at minimum, answer the following basic questions:

- What is the purpose of this process/procedure?
- Who is responsible for performing each activity?
- How is the process/procedure implemented (e.g., key activities over time)?
- When does the activity start and end (e.g., entry and exit criteria)?
- How often is this activity performed (e.g., frequency)?
- What are the tangible inputs and outputs?

Additional information (such as concepts, definitions, and exceptions) may be included as needed to facilitiate understanding and implementation.

SDLC Handbook and Process Change Procedure

Purpose

The purpose of this procedure is to provide a method for documenting and controlling changes to:

- The processes used to produce software at the United States Customs Service
- The Systems Development Life Cycle (SDLC) Handbook

Rationale For Change

There are many reasons why the SDLC and its associated processes and procedures must change. Two of the most important are:

- To make the SDLC process work more efficiently and effectively for Customs
- To become and remain current with the software industry's "best practices"

Changing Project Processes

This procedure does not limit a specific project from changing its own processes as long as the changes are documented and consistent across the project. Successful changes can be recommended as process improvements for the entire organization using the procedure below.

Sources of Change

- Problems identified from project metrics

  Example: If a significant number of defects related to design issues are found in a system, the analysis or development process could be changed to discover design problems earlier in the life cycle.

- Experience

  Example: An individual has had an experience at another organization that would suggest a way to reduce overall life cycle costs by changing the requirements definition process; Customs could choose to incorporate this into its methods for requirements definition.

Continued on next page

SDLC Handbook and Process Change Procedure, Continued

Sources of Change (continued)

- “Industry Standards”

  Example: A new industry standard for interface documentation could be developed that would ease the use of off-the-shelf components. The SDLC and Customs policies would be changed to incorporate this new standard.

Definitions

Process: Describes “what happens” over time within the organization or project in order to build products that meet standards and requirements in accordance with organization policies. It is a series of activities, events, or phases that take place over time and usually have an identifiable purpose or result.

Procedure: Describes “how-to” or “step-by-step” instructions that implement a process in order to obtain a specified outcome.

Work Product: Any final or intermediate product, service, or result of a process or activity. This includes software code, documents, and systems.

This Activity Begins When ...

A staff member documents a better way of doing something.

Note: It is important to ensure that any proposed change will both:

- Reduce probability of problem occurrence
- Not cause new problems

Key Activities

Step	Action
1	Staff member completes an SDLC and Process Improvement Recommendation (SPIR) Form and forwards it to the SDLC Team cc:Mail box. **Example**: See Template in Volume I, Chapter 17, *Process and Control Documents*.

Continued on next page

SDLC Handbook and Process Change Procedure, Continued

Key Activities (continued)

Step	Action
2	Comments and suggestions for change from all staff are reviewed and validated against current process measures. All staff will be notified via bulletin board message or Notes Mail in advance of the reviews. Comments and suggestions will be obtained from submitted SPIRs, project activities, evaluations, and reviews.
3	Results of this review and the following activities are kept in a SPIR database file for process tracking and reporting.
4	New and revised procedures will be piloted and distributed as a result of the current process review.
5	Measurements and interviews will be used to: • Evaluate the success of the new or changed process/procedure • Update the process This evaluation will be planned and documented.
6	All affected personnel will receive appropriate training in the new process/procedure.
7	Results will be refined and approved processes will be incorporated into the SDLC Handbook on its next release.

Continued on next page

SDLC Handbook and Process Change Procedure, Continued

Key Activities (continued)

Step	Action
8	Projects will implement the new/revised process or procedure according to a plan consistent with project activities, but not later than six months after its approval. **Note:** Documentation begun by a project using a prior version of the SDLC or template will not have to be modified if the project does not require the new format to meet its information needs. The SDLC Handbook version/date used for project deliverables should be documented in the Project Plan's Deliverables section.
9	The original submitters will be kept informed of the receipt, status, and action taken in regards to their comments on a quarterly basis.

Roles and Responsibilities

Role	Responsibilities
All Project Team / OIT members, users, and Process Owners	All staff are responsible for making suggestions and comments on processes and procedures used.
Process Improvement Review Team (e.g., from Software Engineering Process Group [SEPG], Process Action Team [PAT], or SDLC work groups)	• Reviews suggestions and comments • Provides feedback to submitters quarterly • Maintains SPIR Project/Status database • Evaluates, recommends, and provides updates to the appropriate Process Guide or SDLC Handbook
Process Owner and Senior Management	• Approves revisions and new procedures • Encourages implementation on projects

Continued on next page

SDLC Handbook and Process Change Procedure, Continued

Roles and Responsibilities (continued)

Role	Responsibilities
Project Managers	• Implementing processes and approved changes in a timely manner
Evaluation Team, SDLC/Process Compliance Group, and/or Project Quality Assurance (QA) Team	• Audits process compliance and collects metrics to evaluate changes/impacts • Reports inconsistencies and suggests process improvements • Assists in training and performance of processes

Inputs

Items that are used or modified during this activity are:

- Submitted SPIR from cc:Mail or Notes Mail mailbox
- Results and comments from SEPG or PAT Work Groups, Project Lessons Learned, Information Resources Management Reviews, or SDLC Compliance Reviews
- Independent QA evaluations of project documentation trail and interviews with the Project Management and System Development Team
- SPIR Template
- SPIR Database File

Outputs

This activity will produce the following:

- Responses to suggestions/comments sent to submitter quarterly
- New or revised process/procedure for piloting and implementation
- Updated SPIR database for analysis/reporting
- Revised SDLC for officially approved policy and procedure changes

Continued on next page

SDLC Handbook and Process Change Procedure, Continued

This Activity Is Complete When ...

- A decision is made on the suggestion/revision to a process

AND

- The submitter is informed of the decision

AND

- The SPIR database is updated.

Critical Success Factors

This process is successful when...

- Processes and procedures are being improved on a regular basis
- Suggestions and comments are regularly submitted from all levels of staff
- Staff comments indicate that existing processes and procedures are routinely used easily and properly
- Measures of process activities are used to demonstrate improvement and assist in training staff on procedures
- Updates are adopted into regular routines in an organized manner

Section B
Basic Principles and Standards

Section Overview

This section presents the standards and principles that form the basis for the Customs Systems Development Life Cycle processes.

Benefits of Using A Life Cycle Methodology

The benefits of using a clear, well-defined life cycle methodology increases the probability that:

- The system's performance will meet the user's needs
- Quality products are developed and maintained
- Resource use is optimized during development
- Systems will comply with relevant standards and regulations
- Efficient and effective applications will be built and implemented
- Risk will be accurately assessed and minimized
- The development process will produce a complete set of deliverables

In This Section

SDLC Principles

User Primacy

Every system development project begins and ends with the user. Application systems development focuses on satisfying user requirements.

Goal

Every phase in the SDLC should be performed with the goal of satisfying the needs of those who will ultimately use and maintain the system.

Successful Project Development

Successful project development requires effective management to ensure the application is developed on schedule, within budget, and produces the expected results.

Effective Project Management

Project management provides a framework that assists the Project Manager in directing all life cycle activities and in making logical estimates of resources, costs, and schedules. Even a small project demands that the project be appropriately managed. Effective project management requires:

- A business sponsor
- A project manager
- The right people on the project team with clearly defined roles, objectives, and responsibilities
- The right tools to accomplish the tasks
- A solid, effective communication mechanism for reporting progress, identifying issues, and sharing lessons learned

Practice Productivity Management

Productivity Management emphasizes the management and leadership of people. It emphasizes managing the environment in which the computer systems are developed.

Although technical proficiency is essential, productivity management recognizes that proper planning, clear role identification, and the implementation of a well-defined process also contribute greatly to project success.

Continued on next page

SDLC Principles, Continued

Practice Productivity Management (continued)

Note: A good technical team member will always plan and manage his/her own productivity even if there is no direct management on a specific task.

Best Practices for Productivity Management

The following principles are incorporated throughout the activities and processes identified in this SDLC Handbook.

- **Capture and Prioritize Work/Project Requests Formally.** This should be done at the appropriate organizational level and should be based upon solid cost/return analysis and mission criticality.
- **Establish a Formal Change Process**. This is essential in order to control project scope and facilitate re-prioritization, re-estimating, and rescheduling efforts.
- **User Involvement Is a Major Productivity Tool**. Involve the user throughout the project, not just at initiation. Begin, collaborate, and end with the end user.
- **Use Automated Tools to Plan, Schedule and Track the Project.** These tools will facilitate tracking project effort, duration, costs, and quality levels.
- **Document and Track Intra-Project Issues, Problems, and Changes Formally.** An application development organization should consistently employ a change management process to control project scope and facilitate re-prioritization, re-estimating and rescheduling efforts. This change management process can be supported by either a project notebook, database, or, preferably, a process management tool.
- **Use the 80-Hour Rule.** Break the job down into "tasks" that require no more than 80 hours to complete. This will also allow effective progress monitoring so that a potential schedule/cost overrun can be caught and corrective actions taken before it becomes a problem.
- **Use Formal and Proven Techniques to Track the Project.** Assign milestones to break the project into smaller, more manageable units. Gather actual information, then use the actuals to re-plan the project on a regular basis.

Policies and Standards

Overview

The following policies and standards apply to **ALL** telecommunications or automated information systems that are owned, leased, or operated by or on behalf of the United States Customs Service.

Government Sources

This handbook is based on extensive research of government standards that apply to Customs SDLC processes. Summaries of these publications are provided in Volume I, Appendix B, *References*.

Treasury Standards Hierarchy

Systems Covered: Treasury Directive TD-87-01, *Information Systems Standards Program*, requires that all Treasury and subordinate agencies Automated Information Systems comply with all mandatory and voluntary standards and guidelines.

Exceptions: Approvals for exceptions must be coordinated through the OIT Program Management Staff (PMS) and the Assistant Commissioner, OIT. The Secretary of the Treasury must approve deviations from Treasury Standards.

FIPS

Systems Covered: Federal Information Processing Standards (FIPS) will be observed by all projects under U.S. Customs auspices.

Exceptions: Approvals for exceptions must be coordinated through the PMS and the Assistant Commissioner, OIT. Exceptions to the FIPS can be granted by the Secretary of Commerce, as stipulated in individual FIPS, under two conditions:

- If the standard would interfere with performance of the organization's mission
- If the cost of implementing the standard would exceed government-wide savings

Continued on next page

Policies and Standards, Continued

Privacy Act and FOIA

Much of the information collected by Customs is covered by either the Privacy Act or the Freedom of Information Act (FOIA).

- For all applications containing information covered by the Privacy Act, a notice should be put in the Federal Register. Contact the Office of Chief Counsel for assistance.
- For information that may be covered under the FOIA, contact the Office of Chief Counsel for assistance in dealing with potential legal issues.

Security Policies

Key References: The key IT security policy reference documents include:

- Treasury *Security Manual*, TD P 71-10
- Treasury *Risk Assessment Guideline*, TD P 85-03
- *Automated Information Systems Security Policy*, CIS HB 1400-05
- Paragraph 4.4 in *USCS Infrastructure and Network Systems Management (NSM) Services Technical Architecture*

Selected overarching IT security policies are listed below.

Access: The most restrictive set of access privileges needed for the performance of authorized tasks will be granted in order to protect sensitive information processed, stored, and/or transmitted by Customs AISs and to protect Customs AIS resources.

Accreditation: Security Certification and Security Accreditation: The security of each AIS in USCS must be both certified and accredited before implementation.

Connectivity: Connectivity between internal Customs AISs and all other systems or networks not covered under Customs Management authority is prohibited without approval of the appropriate Customs accrediting authority.

Continued on next page

Policies and Standards, Continued

Security Policies (continued)

Privacy: All Customs AISs are for official business only. System users should have no expectation of privacy while utilizing these resources, except in so far as privacy requirements have been formally defined, validated, and implemented in a particular AIS.

Process for Exceptions: Any exceptions to the above stated security policies must be thoroughly documented and approved by the Director, AIS Security Division, and by the Assistant Commissioner, OIT.

Disaster Recovery/ Contingency Planning

Disaster Recovery and Contingency Planning is done for all IT systems within Customs. Responsibilities for disaster recovery and contingency planning are as follow:

- Customs field sites are responsible for developing disaster recovery plans that address disasters at their sites or the prolonged unavailability of their local IT systems.
- Mainframe application contingency plans must function within established disaster recovery procedures developed and maintained by the Newington Data Center (NDC).
- NDC’s Applications Development personnel will review any checkpoint restart capabilities designed into the application
- NDC’s Data Administration personnel will also review the software in relation to recovery of data base files, tables, etc.
- For non-mainframe applications, data recovery and alternate site plans should be developed jointly between the developer and User Manager.
- For non-mainframe applications, backup manual procedures are the responsibility of the User Manager.
- Core Business and Mission Support Process Owners are responsible for developing and maintaining their own contingency plans to deal with business continuity issues and risks.

Continued on next page

Policies and Standards, Continued

Graphical User Interfaces

Description: A single standard for graphical user interface (GUI) development has been adopted by the Office of Information and Technology. This is done in order to promote visual and functional consistency within and across GUI applications. The standard describes the components of a GUI and explains design principles for software developers and designers.

Location: The standard is published in the GUI Guidelines Help File, which can be accessed on the LAN. (Y:\GUI)

Process for Exceptions: Rules in the standard are mandatory, recommendations are optional. To obtain an exception or to propose an enhancement, the forms on pages 125 and/or 126 of the GUI Guideline Manual, located with the GUI Guidelines Help File, must be filled out and approved by the Technical Architecture Group (TAG), pending the results of the forthcoming reorganization.

Object-Oriented Technology

There will be both a functional baseline and an allocated baseline as parts of the project documentation for each project which uses OO technology.

These baseline diagrams are considered mandatory deliverables and will be due at the end of the Design phase for each release of the system.

If the project is a maintenance project on an existing system, the baseline documents and the system documentation will be updated appropriately.

Procedure for Exemptions: There are no exemptions from this policy.

Reference: Volume I, Chapter 11, Section E, *Object-Oriented (OO) Technology*

Continued on next page

Policies and Standards, Continued

Architecture Standards

Policy:

- All projects will comply with existing *U.S. Customs Technology Architecture* standards. See Volume I, Appendix B, *References*.
- Functional requirements for projects must include all project deployable requirements as well as project development requirements (such as test tools, CASE tools, etc.)

Process for Exception: Projects must demonstrate overwhelming evidence that their functional requirements warrant exceptions from existing Customs standards. Should a project have a functional requirement not covered by the standard, the Project Manager will work with the support teams to develop recommended solutions. Recommendations will be reviewed and either approved or denied in writing by the manager of OIT's Technical Architecture Group (TAG).

Industry Best Practices

Information on "Best Practices" has been gathered from a number of industry sources. These references are also included in Volume I, Appendix B.

Software Engineering Institute

Customs has made the commitment to reach Level 3 of the SEI's Software Capability Maturity Model (CMM) by 2003. With that goal in mind, "Best Practices" from the CMM have also been incorporated into the Customs SDLC.

Functional Impact Areas

Rationale for Consideration

Projects must ensure that regular communication is maintained between the project and appropriate OIT support organizations. This is critical for:

- Resource Planning
- Cost Estimation
- Project Support/Deliverables Scheduling
- Project Impacts on Other Areas
- A successful implementation

Support Areas Overview

The functional support areas listed below are suggestions for the PM's consideration concerning:

- Possible resources and support functional areas required **by** the project and
- Potential impacts **of** the project on other groups performing these functions.

References:

- Volume I, Chapter 17, *Process and Control Documents,* for a checklist containing these suggestions and allowing project-specific additions

- Volume I, Chapter 4, Section C, **Reporting Across OIT Organizations**.

Note

These functional area names are not meant to indicate organizational groups within OIT; the proper contact's organizational location may change, but the project must still coordinate with the functional group contacts.

Systems Operations-related Areas

- Mainframe Support (all aspects including hardware, software, processing, administration, etc.)
- Centralized Unix Server Support (all aspects)
- Field Unix Server Support (all aspects)
- Communications/Network (all data transfer aspects)
- Voice Communications (Telecom Lines/Dial tone)
- LAN Support (all aspects)
- Storage Management (DASD and Tape)
- System Services (CICS, JES2, MVS, MQM, etc.)

Continued on next page

Functional Impact Areas, Continued

Systems Operations-related Areas (continued)

- Capacity Planning
- Electronic Data Interchange (EDI) Support
- Client/Server Deployment (field equipment, installation, training issues)
- Operations/Scheduling

Data-related Areas

- Database Administration/Support
- Data Administration
- Data Quality Assurance
- Data Conversion
- Corporate Data Dictionary
- Data Warehouse

Standards/ Oversight-related Areas

- Architecture Design/Oversight
- SDLC Compliance/Oversight
- User Interface Standards/Oversight (CICS, GUI)
- Post-Implementation Evaluation/Reviews

Applications/ System Interfaces

- Other Related Projects
- Interfaces with non-Customs Systems, Agencies
- Additional Contract Support (list type)
- Other Support (list type)

Other Functional Areas

- AIS Security
- Procurement
- Configuration Management
  - Development
  - Acceptance Testing
  - Production
- System Acceptance Testing
- User Training
- User Documentation
- Help Desk Support / Customer Support

Section C
Tailoring Guidelines

Section Overview

The goal of the SDLC is to support simplicity, flexibility, and quality throughout the system life cycle. In some circumstances, the SDLC model may not fit the specifics of the development project. **In those cases, the Project Manager, with the concurrence of the Business Sponsor, must adapt SDLC practices to meet the project's unique situations.**

In this section, the parameters for tailoring Customs Automated Information Systems Projects will be outlined. An example of tailoring decisions that can be made using the required Security deliverables/information is also provided.

Previous SDLC Versions

Each project plan should state which version of the SDLC Handbook the project is using, especially for deliverables. The citation should include the handbook title, the complete CIS number and the publication date.

Example: *Systems Development Life Cycle Handbook*, CIS HB 5500-06, October 1996.

In This Section

Documentation

Purpose

Documentation serves three important purposes:

- It preserves information necessary to evolve and maintain the system throughout it's entire useful lifespan or to mitigate risks.
- It provides a mechanism to communicate requirements to the users, the developers, and the testers.
- It provides a means for evaluating the effort required for producing the system and for tracking changes to the system.

Types

There are two types of documentation:

- System documentation used to develop and maintain the application or system
- Project documentation used to monitor and manage the development process

Content

When the project manager makes any modifications to the SDLC methodology, the Project Manager must document:

- WHAT changes were made to the SDLC practices
- WHY the changes were made

Documentation begun by a project using a prior template or version of the SDLC Handbook will not have to be modified if the project does not require the new format to meet its information needs.

Repository

At the beginning of a project, a project file must be established as a repository for all project-related information which should be retained for reference, substantiation, explanation, or clarification as the project progresses.

Continued on next page

Documentation, Continued

Security Documentation

Security requirements may impose additional tailoring criteria based on data sensitivity, processing volume, etc.

Reference: *Automated Information Security Systems Policy*, CIS HB 1400-05, June 1996

Exceptions

- Documentation required for testing and training can only be waived with the explicit approval of the appropriate Division Director or the Assistant Commissioner, OIT.
- Documentation required for security can only be waived with the explicit approval of the appropriate Approval Authorities.

Project Size

Introduction

Customs has divided software development and operational projects into two categories, based on specific characteristics of the project.

Project Categories

Characteristics	IRB Approval	Others
Project Size	Large	Small to Mid-Size
IRB Approval Required?	Yes	Approved by a process to be established by AC, OIT
Cost	$1 million or more	Less than $1 million
Other Factors	High Risk High Visibility Broad, Cross-Organizational Functionality	Low Risk Lower Visibility Single Functional Area Support
Treasury Approval	Treasury approval may be required on any project that has high risk or high visibility, regardless of costs.	

For purposes of simplicity, these distinctions are often summarized as "large projects" (those projects requiring IRB approval) and "smaller projects" (those projects not requiring IRB approval).

Reference: Volume I, Chapter 6, *Project Initiation*

IRB Projects Special Requirements

Projects subject to IRB review and approval require a full, formal Cost/Benefit Analysis. The Cost/Benefit methodology may be tailored for smaller projects.

References:

- Volume I, Chapter 6, *Project Initiation*
- *U.S. Customs Service Cost/Benefit Analysis Workbook*, June 1998
- *Customs IT Investment Management Process*, August 1997

Continued on next page

Project Size, Continued

Other Projects Requirements

For smaller projects, it is possible to abridge many of the deliverables specified in the life cycles.

Example: See Table 12-3, *SDLC Deliverables -- Create, Update/Revise, Finalize*, in Volume I, Chapter 12, *SDLC Deliverables Summary Tables*.

NOTE: It is mandatory that all changes to the SDLC practices be documented. Topics are included in Project Plan Guidelines in Secton B of Volume II, Chapter 13, *Planning Documents*, for suggested methods to document tailoring.

Life Cycle Tailoring

Introduction

There are certain tailoring parameters that must be observed depending on the life cycle chosen.

Waterfall Life Cycle

It is expected that most projects employing this life cycle will be:

- Smaller (non-IRB) projects
- Maintenance projects

References:

- Volume II, Chapter 7, *Traditional Waterfall Life Cycle*
- Volume I, Chapter 12, *SDLC Deliverables Summary Tables*
    - Table 12-2, *SDLC Deliverables -- Functional Team Responsibilities*
    - Table 12-3, *SDLC Deliverables -- Create, Update/Revise, Finalize*

Incremental Life Cycle

Because it breaks large projects down into releases, it is expected that most projects requiring IRB approval will use the Incremental Life Cycle.

Reference: Volume II, Chapter 8, *Incremental Life Cycle*

Information Engineering

Because it addresses business process reengineering during the first three stages of the life cycle, it is expected that Information Engineering will be used only on projects requiring IRB approval.

References:

- Volume II, Chapter 9, *Information Engineering Life Cycle*
- Volume I, Chapter 12, Table 12-4, *Information Engineering Deliverables*

Off-the-Shelf Applications

Projects may use the Commercial Off-the-Shelf (COTS) life cycle as the primary definition for the project, or as part of another life cycle which includes selection and deployment of COTS products. Projects may be of any size, with IRB approval being determined in large part by product costs.

Reference: Volume II, Chapter 10, *Off-the-Shelf (COTS) Applications*

Methodologies

Introduction

Each development methodology has its own tailoring requirements. See the discussions referenced for determining advantages, disadvantages, and life cycle considerations of each.

Object-Oriented

It is expected that initial projects will require IRB approval. As the amount of object-oriented code within the Customs environment grows, smaller projects may also occur.

Reference: Volume I, Chapter 11, Section E, *Object-Oriented (OO) Technology*

Rapid Application Development

It is expected that Rapid Application Development (RAD) projects will require IRB approval, given the amount of planning, resources, and time blockings associated with such projects.

Reference: Volume I, Chapter 11, Section D, *Rapid Application Development*

Joint Application Development

Joint Application Development (JAD) techniques can be used on projects of all types and life cycles. If JAD team members are required to travel, projects using JAD will most likely require IRB approval, due to the impact of travel costs.

References: Volume I, Chapter 11, Section B, *Joint Application Development (JAD)*

Prototyping

Prototyping techniques may be used in projects of all sizes and life cycles.

Reference: Volume I, Chapter 11, Section A, *Prototyping*

Tailoring Security Deliverables

Introduction

As described in Volume II, Chapter 15, there are 22 separate SDLC deliverables needed to provide required security information. However, in actual practice, there will rarely be 22 separate security documents for one project.

Tailoring Options

While collection of the security information included in these 22 deliverables is mandatory for all projects, it is often reasonable to reduce the number of separate deliverables for smaller projects. This can be accomplished in three ways:

- Combining multiple security documents into one document

  Examples of possible combinations:

  - The Security Plan and the Security Test Plan
  - The Security Risk Assessment and the Security Test Report

- Integrating the mandated security information into documents not dedicated to security.

  Examples of plan integration:

  - The Security Test Plan with the System Test Plan
  - The Security Design with the System Design
  - Security Features User's Guide with the User Documentation

Continued on next page

Tailoring Security Deliverables, Continued

Tailoring Options (continued)

- Referencing security-relevant paragraphs in other systems documents

  Examples:

  - Referencing the security-relevant sections of the Functional Requirements under Sections 2.0, 3.0, and 5.0 of the Security Plan
  - Referencing security-relevant sections of the System Test Plan in the Security Test Plan.

  Note: The pointers must appear under the appropriate subparagraphs in the security document and point to the specific subparagraphs in the other system document.

The Minimum Set -- Pre-Operations

The minimum set of separate security documents prior to implementation (that is during the pre-operations phases) for small projects at Customs consists of:

- Security Plan
- Security Risk Assessment
- Security Certification Package
- Security Accreditation Statement

When this minimum set is used, each of these documents must be altered to ensure that the topics/sections below are included.

Security Plan

All topics listed below must be addressed in the Security Plan for all projects. In cases where the topic is sufficiently addressed elsewhere, a reference pointer can be placed in the Security Plan instead of repeating the information.

Security Plan Topic...	May Point To
Security of the Development Process	Project Plan, Section 4.7
Incorporation of the appropriate security features into the application and/or infrastructure	Project Plan, Section 4.0
Production of the appropriate management reports of security planning activity	(no reference pointer)

Continued on next page

Tailoring Security Deliverables, Continued

Security Plan (continued)

Security Plan Topic...	May Point To
Work breakdown for security during development	Project Plan, Sections 3.0 and 4.0
Functional security requirements	Functional Requirements, Section 7.0
Non-functional security requirements (such as those derived from an evolving design)	(no reference pointer)
Security design and/or architecture	System Design, Sections 2.5 and 2.6, or Security Design
System interfaces with other applications and with infrastructure	System Design, Section 2.4, or Security Design document
Security-relevant rules of behavior for users and administrators	Security Plan, Section 3.0
Plan for testing security-relevant features	Security Test Plan, Sections 2.0 and 3.0
Configuration Plan for both hardware and software	Configuration Management Plan, Sections 2.0 and 3.0
Trusted facility policies and procedures	Trusted Facility Manual, Section 3.0
User's guide to security	User Documentation
Disaster recovery policies and procedures	Disaster Recovery/Contingency Plan, Sections 2.0 and 5.0
Contingency planning policies and procedures	Disaster Recovery/Contingency Plan, Sections 2.0 and 5.0
Security training plan	Training Plan, Sections 1.2.7 and 2.3

Note: In cases (e.g., small projects) where the referenced document is optional or does not exist, the topic must be discussed in the Security Plan itself.

Continued on next page

Tailoring Security Deliverables, Continued

Security Risk Assessment

The following topics must be included the Security Risk Assessment with the appropriate information provided either by explicit discussion or by reference:

Security Risk Assessment Topic...	May Point To
Procedures for assessing security risks	Project Plan, Section 2.4
Results of the risk assessment	Security Plan, Section 4.0
Extent of compliance with system vendor recommendations	(no reference pointer)
Security test report, showing the results	Security Test Report, Sections 1.0 and 4.0

Security Certification Package

The Security Certification Package contains a summary statement by the system developer about the extent to which

- The security requirements have been met
- The application and/or infrastructure is in compliance with all security-relevant directives

This technical evaluation would also have all relevant detailed documents attached, including the Security Plan and the Security Risk Assessment.

No system can be implemented without a Security Certification Statement.

Security Accreditation Statement

The Security Accreditation Statement is a summary statement by top management that they understand and accept any residual security risks.

This risk acceptance should include the Security Certification Statement as an attachment.

No system can be implemented without a Security Accreditation Statement.

Continued on next page

Tailoring Security Deliverables, Continued

Operational Documents

Once the system is implemented or deployed, the existing security documents must be periodically updated, and the system re-accredited every three years.

In addition, there are four additionally required security documents:

- Disaster Recovery/Contingency Plan Test Report
- Application Security Audit Policies, Procedures and Reports
- System/Infrastructure Security Audit Policies, Procedures and Reports
- Security Incident Response Policies, Procedures and Reports

Templates and Guidelines

Templates and guidelines for all security deliverables are covered in Volume II, Chapter 15, *Security Deliverables*.

This page intentionally blank